A VA-79

Reference 2

CIPHERING COMMUNICATION SYSTEM

Publication number: JP6112936

Publication date: 1994-04-22

Inventor: KOYAIZU IKURO

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: ***G09C1/00; H04L9/06; H04L9/08; H04L9/14; H04L12/02;*** **G09C1/00; H04L9/06; H04L9/08; H04L9/14; H04L12/02;** (IPC1-7): H04L9/06; G09C1/00; H04L9/14; H04L12/02

- european:

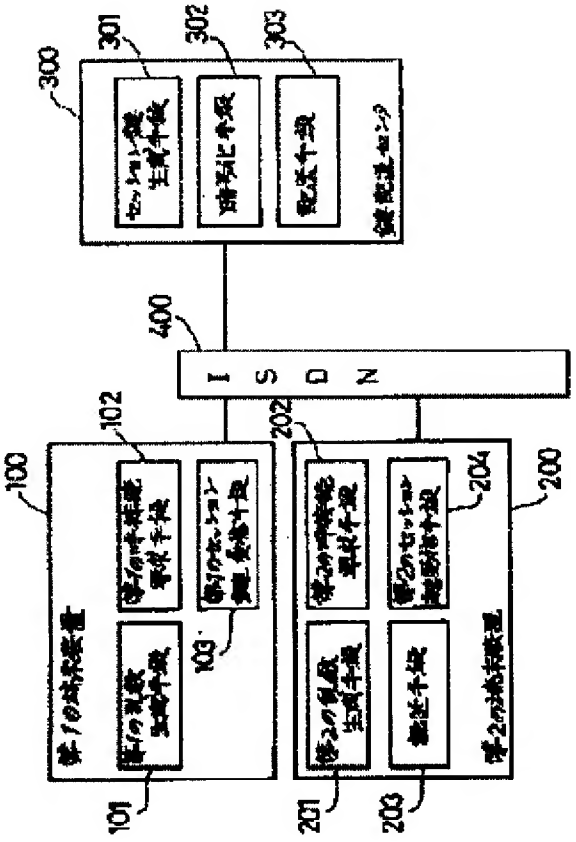
Application number: JP19920262345 19920930

Priority number(s): JP19920262345 19920930

Report a data error here

Abstract of **JP6112936**

PURPOSE:To provide a ciphering communication system of the common key system not requiring complicated key management in which a communication charge of center access is less expensive.
CONSTITUTION:The system is provided with a 1st terminal equipment 100 including a 1st random number generating means 101, a 1st call connection request means 102, and a 1st session key reception means 103, with a 2nd terminal equipment 200 including a 2nd random number generating means 201, a 2nd call connection request means 202, a 2nd session key reception means 204, and a transfer means 203, and with a key delivery center 300 including a session key generating means 301, a ciphering means 302, and a delivery means 303 adding a ciphered signal by the ciphering means 302 to a call number release request message and delivering the result.



AVA-79
2

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－112936

(43)公開日　平成６年(1994)４月22日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		8837－5Ｌ			
			7117－5Ｋ	Ｈ０４Ｌ	9/ 02	Ｚ
			8732－5Ｋ		11/ 02	Ｚ

審査請求　未請求　請求項の数２(全 10 頁)　最終頁に続く

(21)出願番号　特願平4－262345

(22)出願日　平成４年(1992)９月30日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　小柳津　育郎
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

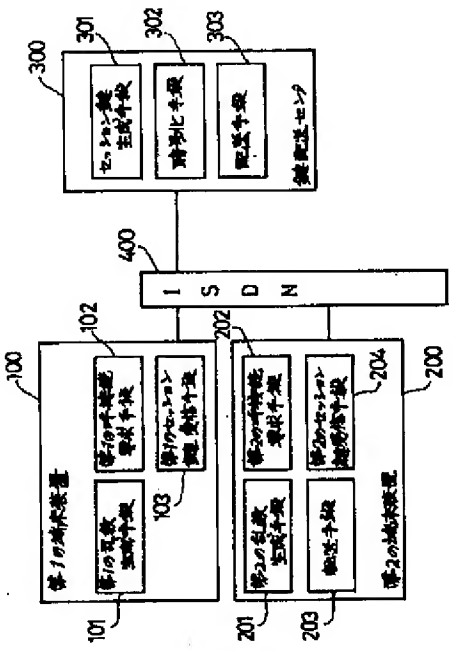
(54)【発明の名称】　秘話通信システム

(57)【要約】

【目的】　本発明の目的は、センタアクセスの通信料が安価で且つ複雑な鍵管理を必要としない共通鍵方式の秘話通信システムを提供することである。

【構成】　本発明は、第１の乱数生成手段１０１と、第１の呼接続要求手段１０２と、第１のセッション鍵受信手段１０３を含む第１の端末装置１００と、第２の乱数生成手段２０１と、第２の呼接続要求手段２０２と、第２のセッション鍵受信手段２０４と、転送手段２０３を含む第２の端末装置２００と、セッション鍵生成手段３０１と、暗号化手段３０２と、暗号化手段３０２により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段３０３を含む鍵配送センタ３００を有する。

本発明の原理構成図



1

【特許請求の範囲】

【請求項１】　ＩＳＤＮ回線に接続される複数の端末装置と鍵配送センタからなり、鍵配送センタから配送されるセッション鍵を用いて暗号通信を行う通信システムにおいて、

第１の乱数を生成する第１の乱数生成手段と、呼設定要求メッセージに自加入者番号と該第１の乱数とを付加して通信相手となる端末装置に呼接続要求する第１の呼接続要求手段と、応答メッセージに付加された前記セッション鍵を受信する第１のセッション鍵受信手段を含む第１の端末装置と、

第２の乱数を生成する第２の乱数生成手段と、呼設定要求メッセージに自加入者番号と該第２の乱数及び前記第１の端末装置の加入者番号と前記第１の乱数を付加して鍵配送センタに呼接続要求する第２の呼接続要求手段と、前記鍵配送センタからの呼解放要求メッセージに付加されたセッション鍵を受信する第２のセッション鍵受信手段と、前記鍵配送センタからの前記セッション鍵を応答メッセージに付加して前記第１の端末装置に転送する転送手段を含む第２の端末装置と、

前記第２の端末装置からの呼設定要求メッセージの第１の端末装置の加入者番号と前記第２の端末装置の加入者番号が登録されている場合にはセッション鍵を生成するセッション鍵生成手段と、該セッション鍵生成手段により生成したセッション鍵と、前記第１の乱数を前記第１の端末装置の暗号鍵で暗号化し、該セッション鍵と前記第２の乱数を前記第２の端末装置の暗号鍵で暗号化する暗号化手段と、該暗号化手段により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段を含む鍵配送センタを有することを特徴とする秘話通信システム。

【請求項２】　前記鍵配送センタに登録されている端末装置の暗号鍵に、暗号鍵を前記鍵配送センタの秘密鍵と秘密パラメータとから生成する暗号鍵生成手段を含む鍵配送センタを有する請求項１記載の秘話通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、共通鍵暗号アルゴリズムを用いてＩＳＤＮ回線に接続した端末装置間で暗号通信を行う場合の秘話通信システムに係り、特に事業所等の複数メンバからなるグループ内で、共通鍵方式の暗号通信を行う場合に好適な秘話通信システムに関する。

【０００２】

【従来の技術】共通鍵暗号アルゴリズムは、暗号文を作成するときの鍵（暗号鍵）と、暗号文を元に戻すときの鍵（復号鍵）に同じ数値データを用いる暗号方式である。この暗号方式を用いて各端末装置が互いに他と秘密の通信を行うには、各端末装置毎に、互いに通信する端末装置数に等しい暗号鍵が必要である。しかしながら、端末装置数が増えれば鍵の数が膨大となる。

2

【０００３】このため、従来、各端末装置が秘密にする暗号鍵を登録しておく鍵配送センタを別に設置し、端末装置＃ｉが端末装置＃ｊと暗号通信を開始する度に鍵配送センタにアクセスして登録してある暗号鍵K_i，K_jで暗号化したセッション鍵を配送して貰う。端末装置＃ｉと端末装置＃ｊは、暗号化されたセッション鍵を互いに復号し、このセッション鍵を用いて以後の通信を暗号化するのが一般的である。

【０００４】

【発明が解決しようとする課題】従来の技術のような鍵配送センタがセッション鍵を配送する方式は、端末装置が管理する鍵は一つでよい。しかし、この方法の第１の問題として、実際の通信に先立って鍵配送センタからセッション鍵を受け取るための通信料が別に必要である。

【０００５】また、第２の問題として、鍵配送センタに端末装置の鍵ファイルが必要であり、第３者がそのファイルへの不法アクセスを防止するために膨大な鍵ファイルを保護された領域に置く必要がある。このため、多数の端末装置を接続し、鍵の書き換えを行う場合などには複雑な鍵管理を行う必要がある。

【０００６】本発明は上記の点に鑑みてなされたもので、センタアクセスの通信料が安価で且つ複雑な鍵管理を必要としない共通鍵方式の秘話通信システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】図１は、本発明の原理構成図である。

【０００８】本発明は、ＩＳＤＮ回線４００に接続される複数の端末装置と鍵配送センタ３００からなり、鍵配送センタ３００から配送されるセッション鍵を用いて暗号通信を行う通信システムにおいて、第１の乱数を生成する第１の乱数生成手段１０１と、呼設定要求メッセージに自加入者番号と第１の乱数とを付加して通信相手となる端末装置に呼接続要求する第１の呼接続要求手段１０２と、応答メッセージに付加されたセッション鍵を受信する第１のセッション鍵受信手段１０３を含む第１の端末装置１００と、第２の乱数を生成する第２の乱数生成手段２０１と、呼設定要求メッセージに自加入者番号と第２の乱数及び第１の端末装置１００の加入者番号と第１の乱数を付加して鍵配送センタ３００に呼接続要求する第２の呼接続要求手段２０２と、鍵配送センタ３００からの呼解放要求メッセージに付加されたセッション鍵を受信する第２のセッション鍵受信手段２０４と、鍵配送センタ３００からのセッション鍵を応答メッセージに付加して第１の端末装置１００に転送する転送手段２０３を含む第２の端末装置２００と、第２の端末装置２００からの呼設定要求メッセージの第１の端末装置１００の加入者番号と第２の端末装置２００の加入者番号が登録されている場合にはセッション鍵を生成するセッション鍵生成手段３０１と、セッション鍵生成手段３０１

により生成したセッション鍵と、第1の乱数を第1の端末装置１００の暗号鍵で暗号化し、セッション鍵と第2の乱数を第２の端末装置２００の暗号鍵で暗号化する暗号化手段３０２と、暗号化手段３０２により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段３０３を含む鍵配送センタ３００を有する。

【０００９】また、本発明は、鍵配送センタ３００に登録されている端末装置に、暗号鍵を鍵配送センタ３００の秘密鍵と秘密パラメータとから生成する暗号鍵生成手段を含む。

【００１０】

【作用】本発明は、端末装置が秘話通信を行う場合には、呼設定要求メッセージに自加入者番号と乱数を付加して、相手端末装置に呼接続要求を行う。要求された端末装置は、呼接続シーケンスを保留したまま、発信端末装置から送られた加入者番号と乱数に自端末装置の加入者番号と乱数を加えたものを呼設定要求メッセージに付加して、鍵配送センタに呼接続要求する。

【００１１】鍵配送センタは、両端末装置が登録されていれば、セッション鍵と両端末装置の暗号鍵を生成し、それぞれの端末装置の暗号鍵で暗号化したセッション鍵と乱数を呼解放要求メッセージに付加して送出する。着信端末装置は、自分と鍵配送センタだけが知る暗号鍵でセッション鍵と自分が生成した乱数を復号し、正しいセッション鍵を受信したことを確認する。次いで、発信端末装置と呼設定シーケンスを再開し、鍵配送センタから受け取った応答メッセージに付加してある暗号化されたセッション鍵と乱数を発信端末装置に転送する。これにより、発信側の端末装置は、鍵配送センタと自分だけが知る暗号鍵を用いて、セッション鍵と最初に送った乱数を復号し、正しいセッション鍵を受信したことを確認することができるため、両端末装置は、受信したセッション鍵を用いて呼設定後の秘話通信を行うことができる。

【００１２】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【００１３】図２は本発明の一実施例の共通鍵暗号アルゴリズムを用いた秘話通信システムのブロック図を示す。

$$K_i = eK_m\ (ID_i \| G_i \| P) \quad *$$

但し、$K_m = K + G_i$

ここで、Kは鍵配送センタ２の秘密鍵、Pは秘密パラメータ（秘密値）を示し、

【数2】

"‖"

【００２０】は連結（concatenation）を示し、"＋"はビット対応の排他的論理和を示す。

【００２１】図３は、本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す。同図中、（ａ）は鍵配送センタの鍵管理テーブルを示し、（ｂ）は端末装置１＃ｉの鍵管理テーブルを示す。この鍵管理テーブルは、端末装置１と鍵配送センタ２が管理する鍵情報を示すものである。

【００２２】同図中（ａ）及び（ｂ）のＳ，Ｓ’で示される部分は外部からのアクセス禁止の秘密情報を示し、鍵配送センタ２の暗号鍵Ｋ及び秘密パラメータＰ及び端末装置１＃ｉの暗号鍵K_iは外部からアクセスできない保護された領域に記憶されている。

【００２３】次に本発明の一実施例のセッション鍵配送手順について説明する。

【００１４】同図において、端末装置１は、ＩＳＤＮ加入者回線のレイヤ１～レイヤ３制御及びレイヤ４から上の上位レイヤのネットワーク制御を行う端末制御部１１と暗号演算部１２と鍵管理テーブル部１３とランダムデータ発生部１４から構成されている。

【００１５】また、鍵配送センタ２は、ＩＳＤＮ加入者回線のレイヤ１～レイヤ３制御及び上位レイヤの鍵配送制御を行うセンタ制御部２１と暗号演算部２２と鍵管理テーブル部２３及びランダムデータ発生部２４から構成されている。暗号演算部１１、暗号演算部２２については、ブロック暗号であれば、どのような暗号アルゴリズムを採用してもよい。代表的なアルゴリズムとしては、ＦＥＡＬ暗号アルゴリズムやＤＥＳ暗号アルゴリズムがある。ＦＥＡＬ暗号アルゴリズムの詳細は、文献「宮口他、ＦＥＡＬ－８暗号アルゴリズム、研実報、Vol.37, No,4/5, ページ321 ～327 、1988年」を、ＤＥＳ暗号アルゴリズムの詳細は文献「小山著、情報セキュリティ、電気書院、ページ76～88、1989年刊行」を参照されたい。暗号演算部２２は暗号鍵とデータを入力として、平文ｐを鍵K_iで暗号化した暗号文eK_i（ｐ），暗号文ｃを鍵K_iで復号した平文dK_i（ｃ）及びデータｄを鍵K_iで暗号化した結果の最後のブロックの上位４バイトｍａｃ（K_i，ｄ）の３種類の演算を実行する。

【００１６】〈端末装置設置時の手続〉次に端末装置設置時の手続について説明する。

【００１７】端末装置１＃ｉを設置するときには、予め次の手続により、端末装置１＃ｉの鍵管理テーブル部１３と鍵配送センタ２の鍵管理テーブル部２３の鍵管理テーブルに次の情報を通信とは別の手段により書き込んでおく。

【００１８】鍵配送センタ２に端末装置１＃ｉの番号ID_iと鍵修飾パラメータG_iを登録する。

【００１９】以下に示す式（１）によりF_iを生成し、最後の８バイトを端末装置１＃ｉの鍵K_iとする。端末装置１＃ｉの鍵管理テーブル部１３に１６バイトの端末装置１＃ｉの加入者番号（公開可能）ID_i，端末装置１＃ｉの鍵修飾パラメータ（公開可能）G_iと鍵K_iを書き込む。

【数１】

…（１）

5

【００２４】図４は本発明の一実施例の呼接続手順を説明するための図を示す。同図（ａ）はＢチャネルを接続し、通話を行う場合を示し、（ｂ）はＢチャネルの接続をしない場合を示す。

【００２５】ＩＳＤＮ加入者線に接続されたディジタル電話機などの端末装置１＃ｉが通信相手の端末装置１＃ｊを呼び出して回線交換の呼接続を行う手順（以下呼接続手順と記す）は図４（ａ）のように行われる。即ち、呼接続は発信者１＃ｉからのＳＥＴＵＰ（呼設定の要求）メッセージの送出により開始される。ＩＳＤＮ網３からの呼設定処理中の意味をもつＣＡＬＬ　ＰＲＯＣ（Call Proceeding:呼設定のための処理中の通知）の転送を経て、着信者１＃ｊの呼出が始まると、ＡＬＥＲＴ（Alerting：着信者を読み出し中の通知）メッセージが発信者１＃ｉに送られる。

【００２６】次に着信側端末装置１＃ｊが応答するとＣＯＮＮ（Connect: 着信者が応答したことを通知）メッセージが発信端末装置１＃ｉに、ＣＯＮＮ　ＡＣＫ（Connect Acknowledge:ＣＯＮＮに対する確認）メッセージがＩＳＤＮ網３から着信端末装置１＃ｊに送られてＢチャネルの接続が完了し、通信が始まる（詳細は、例えば文献：「秋山監修、ＩＳＤＮ絵とき読本、頁92～101 、オーム社、1988年発行」を参照）。

【００２７】また、端末装置１に呼びだされた鍵配送センタ２が呼接続シーケンスの中でセッション鍵を配送するだけで、Ｂチャネルを接続し、以後のデータ通信を行う必要がない場合は（詳細は後述する）、着呼拒否として、図４（ｂ）のように（ａ）に示されるＡＬＥＲＴおよびＣＯＮＮメッセージの代わりに、ＲＥＬ　ＣＯＭＰ（Release Complete:チャネル解放と呼番号解放要求）メッセージで応答して、Ｂチャネルの接続をすることなく、呼接続手順を終了することができる（詳細は、「日本電信電話（株）、技術参考資料、ＩＮＳネットワークサービスのインタフェース　第３分冊、電気通信協会、１９９０年発行」の頁１５２～頁１５３、及び頁１６０～頁１６１を参照）。

【００２８】一方、ＩＳＤＮには、呼設定時のメッセージに付随して、通信を行うユーザ間で比較的短いデータのやりとりができるユーザ・ユーザ信号（User-to-User Singnalling）が付加サービスとして規定されている。

【００２９】図５は本発明の一実施例の呼設定要求メッセージの形式を示す。同図（ａ）は、本付加サービスを利用する場合の呼設定メッセージの形式を示す。共通部４１の先頭から個別部４２の高位レイヤ整合性までが通常の呼設定時のメッセージで送信される情報であり、ユーザ・ユーザ情報要素が本付加サービスによって転送される情報である。この時、共通部のメッセージタイプは次の表１のメッセージを用いることができる。

【００３０】

【表１】

6

SETUP	０００００１０１
ALERT	０００００００１０
CONN	０００００１１１
DISC	０１０００１０１
REL	０１００１１０１
REL　COMP	０１０１１０１０

各情報要素の詳細及びメッセージタイプに付随する個別部の情報要素の詳細説明は、本発明内容を説明するのに必須ではないので省略するが、詳細は文献：「秋山監修、ＩＳＤＮ絵とき読本、オーム社、１９８８年発行」、或いは「日本電信電話（株）技術参考資料、ＩＳＮネットサービスのインタフェース　第３分冊、電気通信協会、１９９０年発行」などに詳しく述べられている。

【００３１】本発明は、このユーザ・ユーザ信号の付加サービスを利用して鍵配送情報の交換を行う。本発明で使用するユーザ・ユーザ情報要素の形式を図５（ｂ）に示す。ここで、ユーザ・ユーザ情報要素の第１バイトはユーザ・ユーザ情報要素識別子４３で０１１１１１１０、第２バイトは内容長４４であり、第３バイト以下のデータバイト長の値を示す。第３バイトはプロトコル識別子４５であり、本実施例のようにユーザの必要性に応じて情報内容を構成する場合には、ユーザ特有のプロトコルを表す“００００００００”を入れることが決められている（詳細は、文献「日本電信電話（株）技術参考資料、ＩＮＳネットサービスのインタフェース、第３分冊、電気通信協会、１９９０年発行」のページ１２２～１２３を参照）。第４バイトは、本発明の実施例で定義する表２に示すコマンド４６、第５バイトは内容長４７で以後の鍵情報の長さを示すバイト数、第６バイト以降に鍵情報４８が格納される。

【表２】

コマンド

Ｑ１：暗号化要求	１００００００００
Ｑ２：暗号化不能	１００００００１
Ｑ３：暗号化失敗	１００００００１０

なお、図４（ｂ）の“ＲＥＬ　ＣＯＭＰ”メッセージは網によってＤＩＳＣ（Disconnect: 呼解放要求）メッセージに変換されて発信端末装置１＃ｊに解放要求として通知されるが、“ＲＥＬ　ＣＯＭＰ”メッセージに付加したユーザ・ユーザ情報はＤＩＳＣメッセージにそのまま付加されて発信端末装置１＃ｉに転送される（詳細は、「日本電信電話（株）、技術参考資料、ＩＮＳネットサービスのインタフェース第３分冊、電気通信協会、１９９０年発行」の頁１８５を参照）。

7

【0032】〈通信時の手続き〉次に、通信時の手続きについて説明する。本実施例では、端末装置1＃iが端末装置1＃jを呼び出して暗号通信する際の鍵共有手続きを説明する。

【0033】図6は、本発明の一実施例のセッション鍵配送のためのISDN呼接続手順を示す。

【0034】（a）端末装置1＃iはランダムデータ発生部14を起動し、乱数R_iを生成する。鍵管理テーブル部12から加入者番号ID_i、鍵修飾パラメータG_iを読み出す。次に端末制御部11を起動し、呼設定シーケンスのSETUPメッセージのユーザ・ユーザ情報要素の第2バイトの内容長44を35にセットし、第4バイト以降に暗号化要求コマンドQ1，内容長32、加入者番号ID_i、鍵修飾パラメータG_i、乱数R_iを付加して、端末装置1＃jに送信する（図6①）。以降の説明では第2バイトの内容長44の記述は省略する。

【0035】（b）着信端末装置1＃jの端末制御部11は、発信端末装置1＃iからSETUPメッセージを受信すると、SETUPメッセージのユーザ・ユーザ情報の中身を解析し、暗号化要求コマンドQ1があると、ランダムデータ発生部14を起動し、乱数R_jを生成する。鍵管理テーブル部12から加入者番号ID_i、鍵修飾パラメータG_iを読み出す。続いて、次のメッセージ*

8

*をSETUPメッセージのユーザ・ユーザ情報要素を用いて鍵配送センタ2へ送信する（図6②）。このとき、ユーザ・ユーザ情報要素のメッセージとしては、暗号化要求コマンドQ1，内容長64、加入者番号ID_i、鍵修飾パラメータG_i、乱数R_i、着信端末装置1＃jの加入者番号ID_j、着信端末1＃jの鍵修飾パラメータG_j、着信端末1＃jの乱数R_jである。

【0036】（c）鍵配送センタ2がSETUPメッセージを受信すると、センタ制御部21がSETUPメッセージを解析し、暗号化要求コマンドを検知すると、加入者番号ID_i及び鍵修飾パラメータG_jとから鍵管理テーブル部23を検索し、対応する加入者の鍵修飾パラメータG_i及びG_jが登録されているかどうか検査する。受信した鍵修飾パラメータと登録されている鍵修飾パラメータが一致していれば、鍵配送センタ2は、ランダムデータ発生部24を起動して、8バイトのランダムデータを発生させ、セッション鍵K_sとする。鍵配送センタ2は、暗号演算部22を起動し、前述の式（1）によりセッション鍵K_i、K_jを生成し、C_1，C_2、検証コードMAC$_1$，MAC$_2$を計算する。但し、$C_1 = eK_i(K_s)$，$C_2 = eK_j(K_s)$，

【数3】

$$MAC_1 = mac(K_i, ID_i \| G_i \| C_1 \| R_i \|).$$

$$MAC_2 = mac(K_j, ID_j \| G_j \| C_2 \| R_j \|).$$

である。上記のMAC（Message Authentication Code）は送信者と受信者間で暗号鍵K_iを共有する場合にだけ同じ結果が得られることから、データdが通信途中で改ざんされていないことを検証するために利用されるコードである。

【0037】次に、センタ制御部21は呼設定シーケンスのREL COMPメッセージのユーザ・ユーザ情報要素を用いて以下のメッセージを端末装置1＃jに応答する（図6③）。ユーザ・ユーザ情報要素のメッセージとしては、暗号化要求コマンドQ1，内容長24、鍵K_iで暗号化した暗号文C_1、検証コードMAC$_1$，鍵K_jで暗号化した暗号文C_2，検証コードMAC$_2$である。

※【0038】もし、加入者番号ID_i，ID_jのいずれかが登録されていない、あるいは登録されている番号ID_iと鍵修飾パラメータG_iが一致しない等の異常が発見された場合は、呼設定シーケンスのREL COMPメッセージのユーザ・ユーザ情報要素を用いてQ2（暗号化不能）メッセージを端末装置1＃jに応答する。

【0039】（d）端末装置1＃jは、DISCメッセージを受信し、暗号要求コマンドを検出すると、鍵管理テーブル部13から自己の暗号鍵K_jを暗号演算部12に与えて、セッション鍵K_sと検証コードMAC$_2$'を計算する。

【数4】

※

$$K_s = dK_j(C_2)$$

$$MAC_2' = mac(K_j, ID_j \| G_j \| C_2 \| R_j)$$

MAC$_2$ =MAC$_2$'ならば、セッション鍵K_sが正しいと確認し、セッション鍵K_sを得る。続いて、端末装置1＃jは、暗号演算部12にセッション鍵K_sと手順★

★（b）で端末装置1＃iから受信した情報ID_i，G_i及びR_iを与えて、

【数5】

$$MAC_3 = mac(K_s, ID_i \| G_i \| R_i)$$

を計算し、CONNメッセージのユーザ・ユーザ情報要素を用いて、鍵配送センタから受信した鍵情報｛C_1，MAC$_1$｝に付加し、暗号化要求コマンドQ1，内容長16、鍵K_iで暗号化した暗号文C_1、検証コードMAC$_3$のメッセージを端末装置1＃iに送信する（図6④）。もし、鍵配送センタ2からQ2（暗号化不能）メッセージを受信するか、または、MAC$_2$ ≠MAC$_2$'ならば、CONNメッセージのユー

9

ザ・ユーザ情報要素を用いて、Ｑ３メッセージを端末装置１＃ｉに返送し、鍵共有手続きが失敗したことを通知する。なお、セキュリティシステム上失敗の原因はメッセージ内に詳述しない。

【００４０】（ｅ）端末装置１＃ｉはＣＯＮＮメッセー＊

10

＊ジを受信すると、ユーザ。ユーザ情報要素を解析する。暗号要求コマンドＱ１があれば、自端末装置のを暗号演算部１２に暗号鍵を与えて、

【数６】

$$K_s = dK_i\ (C_i)$$

$$MAC_i' = mac\ (K_i,\ ID_i \| G_i \| C_i \| R_i)$$

【００４１】を計算する。また、暗号演算部１２に結果のセッション鍵K_sを与えて、

※【数７】

$$MAC_3' = mac\ (K_s,\ ID_i \| G_i \| R_i)$$

を求める。$MAC_1 = MAC_1'$且つ$MAC_3 = MAC_3'$ならば、配送されたセッション鍵が鍵配送センタ２から配送されたものであることが証明されるため、端末装置１＃ｊと正しいセッション鍵K_sを共有したことを確認し、呼接続と鍵共有手続きを完了する。

【００４２】端末装置１＃ｉと端末装置１＃ｊは以降のＢチャネル暗号通信をセッション鍵K_sを用いて行う。

【００４３】もし、端末装置１＃ｉが暗号化失敗コマンドＱ３を受信するか、$MAC_1 \neq MAC_1'$か、または、$MAC_3 \neq MAC_3'$であると、鍵配送手順の途中で何らかの不都合が生じたことを示しており、安全のため通信を中断する。

【００４４】

【発明の効果】暗号通信を行う各端末装置のそれぞれが暗号鍵を鍵配送センタに登録しておき、登録された任意の相手と暗号通信を行う場合に、従来の方法では、端末装置は相手の端末装置との暗号通信に先立って、鍵配送センタに１度回線接続してセッション鍵の配送を行う必要があった。このため、従来の方法では、実データの暗号通信に要する通信料のほかに、鍵配送センタからのセッション鍵を受信するために最低でも１度数分の通信料が別に必要となる問題がある。

【００４５】しかしながら、本発明によれば、鍵配送センタと回線接続をせずにセッション鍵の配送を行うため、上記の欠点を解消することができる。また、本発明によれば、鍵配送センタには公開可能な加入者番号と鍵修飾パラメータを登録しておき、鍵配送センタは自己の秘密とする暗号鍵と秘密パラメータから各端末装置の暗号鍵を生成するため、鍵ファイルをもつ必要がなくなる。このため、ただ２つの秘密値を外部からの読み出し禁止にするだけでよい。また、端末装置の移設や、加入者回線を変更した場合には、鍵配送センタの鍵管理テーブルの公開可能な加入者番号または端末装置の鍵修飾パラメータの値を書き換えることによって容易に変更できるため、鍵配送センタの鍵管理が極めて簡単になる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の一実施例の共通鍵暗号アルゴリズムを用いた秘話通信システムのブロック図である。

【図３】本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す図である。

【図４】本発明の一実施例の呼接続手順を説明するための図である。

【図５】本発明の一実施例の呼設定要求メッセージの形式を示す図である。

【図６】本発明の一実施例のセッシン鍵配送のためのＩＳＤＮ呼接続手順を示す図である。

【符号の説明】

１　端末装置
２　鍵配送センタ
３　ＩＳＤＮ網
１１　端末制御部
１２　暗号演算部
１３　鍵管理テーブル
１４　ランダムデータ発生部
２１　センタ制御部
２２　暗号演算部
２３　鍵管理テーブル部
２４　ランダムデータ発生部
４１　共通部
４２　個別部
４３　ユーザ・ユーザ情報要素識別子
４４　内容長
４５　ユーザ特有プロトコル
４６　コマンド
４７　内容長
４８　鍵情報
１００　第１の端末装置
１０１　第１の乱数生成手段
１０２　第１の呼接続要求手段
１０３　第１のセッション鍵受信手段
２００　第２の端末装置
２０１　第２の乱数生成手段
２０２　第２の呼接続要求手段

11

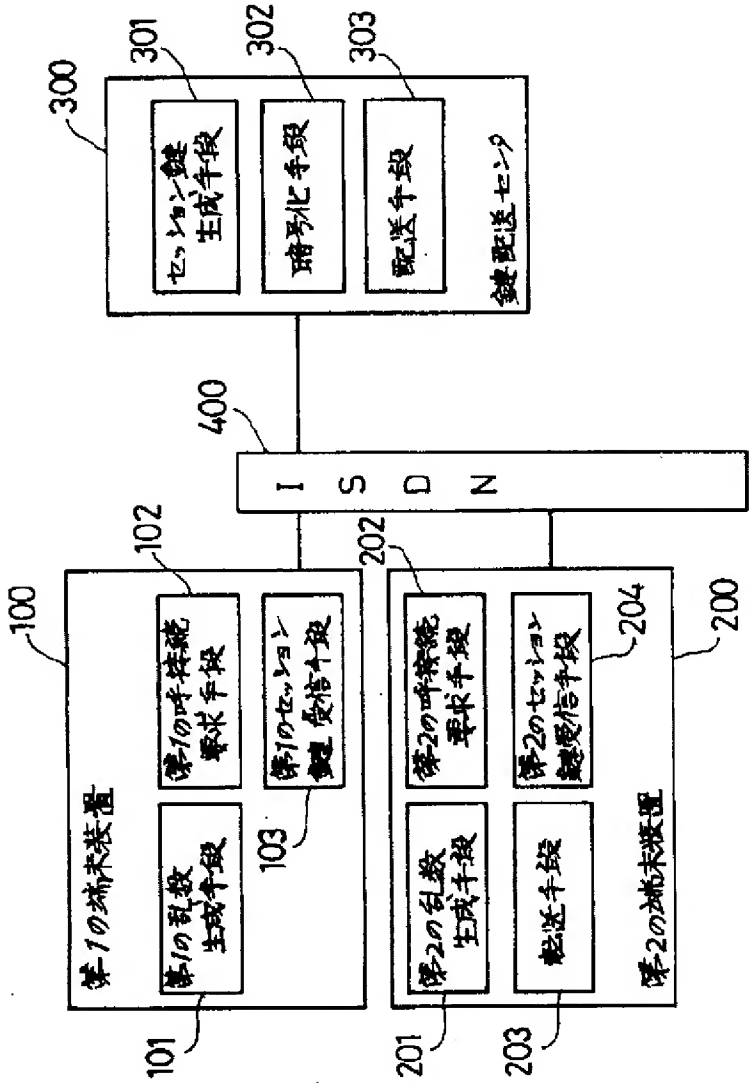
２０３　転送手段
２０４　第２のセッション鍵受信手段
３００　鍵配送センタ
３０１　セッション鍵生成手段

12

３０２　暗号化手段
３０３　配送手段
４００　ＩＳＤＮ網

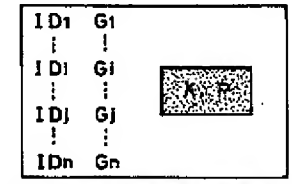
【図１】

本発明の原理構成図



【図３】

本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す図



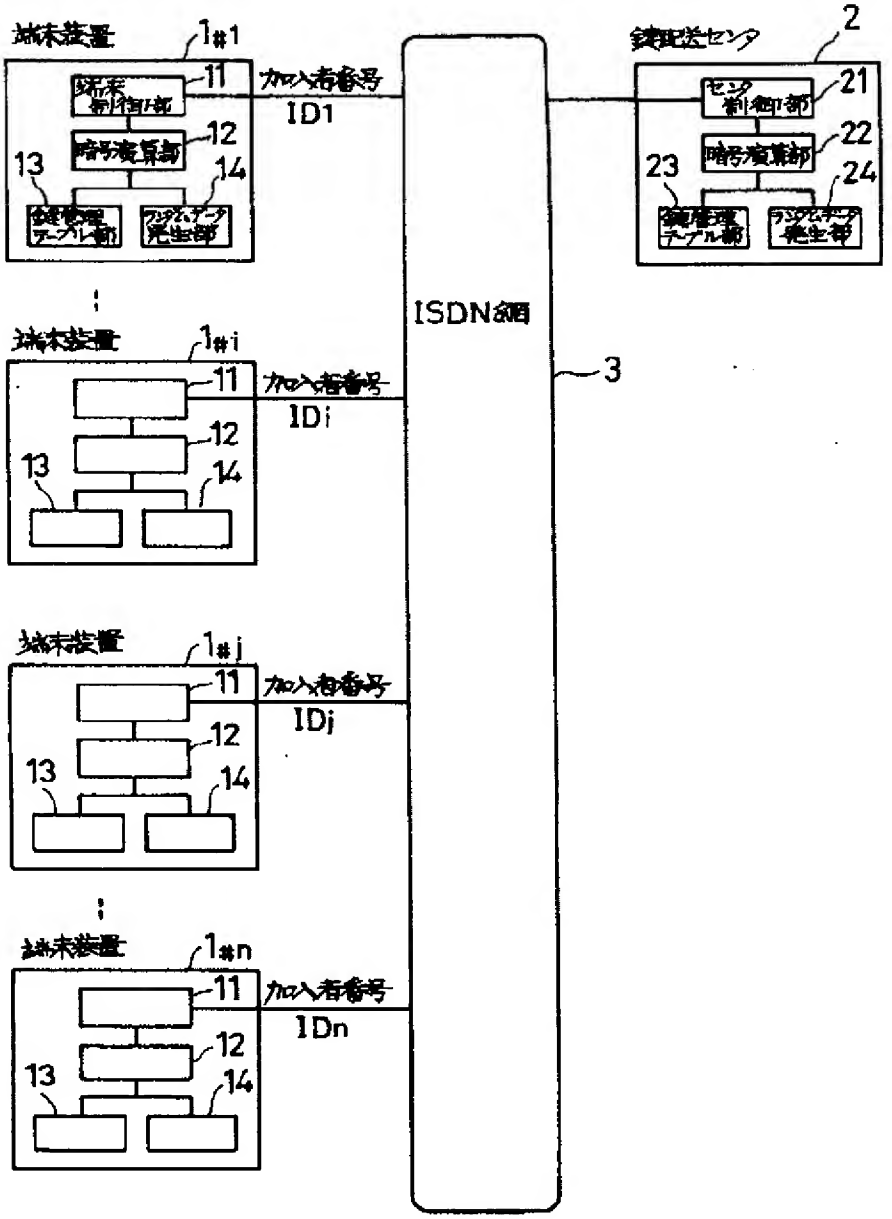
(a) 鍵配送センタの鍵管理テーブル

(b) 端末装置＃iの鍵管理テーブル

：外部からのアクセス禁止の秘密情報

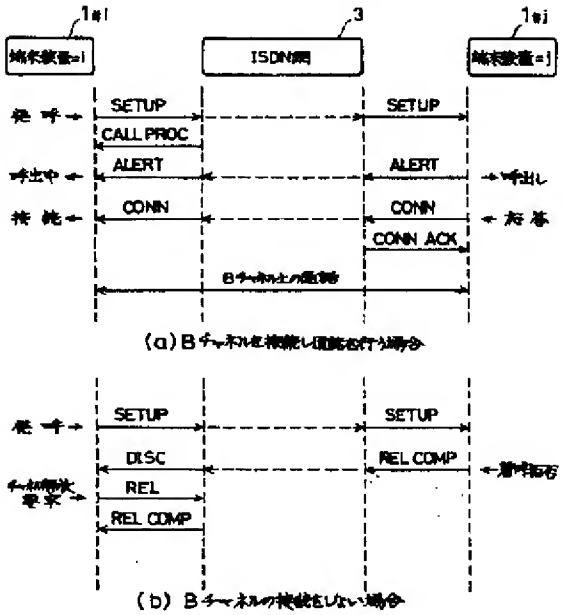
【図2】

本発明の一実施例の共通鍵暗号アルゴリズムを用いた秘話通信システムのブロック図



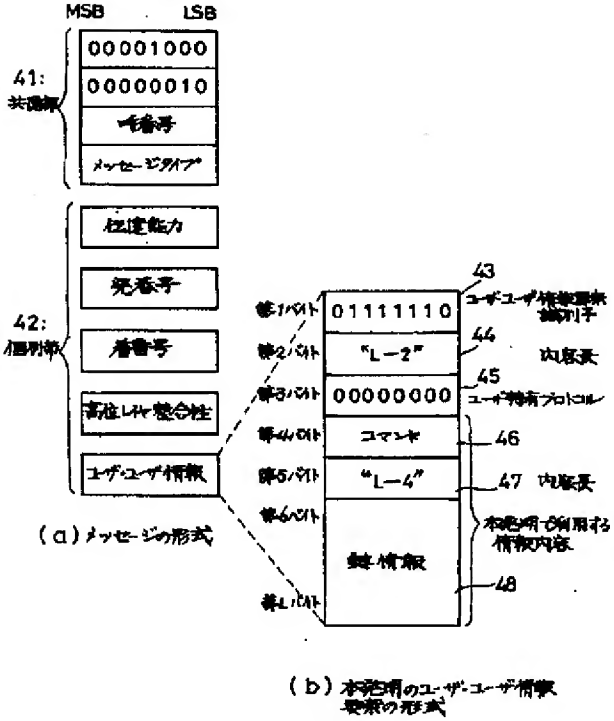
【図４】

本発明の一実施例の呼接続手順を説明するための図



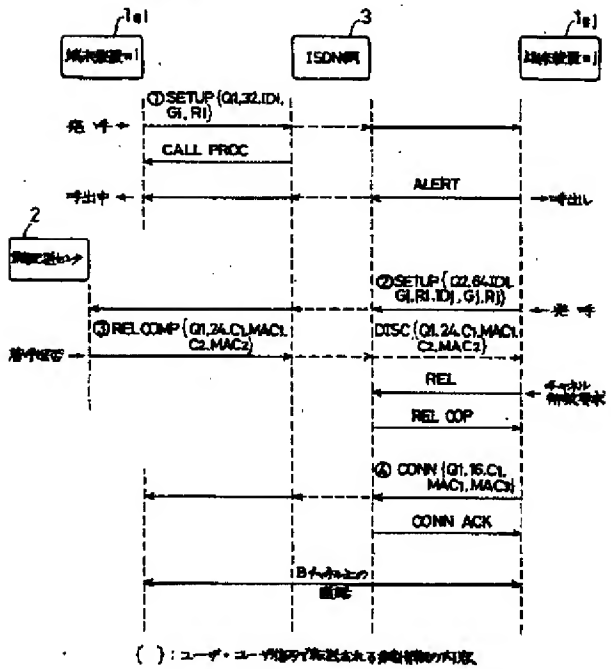
【図５】

呼設定要求メッセージの形式を示す図



【図６】

本発明の一実施例のセッション確立のためISDN呼接続手順を示す図



フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/02				